Listing of Claims:

1. (Currently Amended) An electronic voting method, comprising the ~~step~~ steps of:

obtaining from a signer apparatus, using a fair blind signature scheme, ~~to obtain~~ a digital signature (y_i) of a data signal (x_i) from a voter apparatus, said data signal comprising a ~~voter's~~ vote (v_i) of a voter; and

establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme.

2. (Currently Amended) The voting method of claim 1, wherein the fair blind signature scheme ~~is~~ comprises a threshold fair blind signature scheme in which the digital signature is obtained from a sub-set of a group of servers which form said signer apparatus, the group of servers containing n servers and the sub-set containing t servers, where $t < n$.

3. (Currently Amended) The voting method of claim 1, wherein the data signal (x_i) corresponds to the ~~voter's~~ vote (v_i) of the voter which is encrypted according to a first encryption scheme (E_{TM}), said first encryption scheme being the encryption scheme of a first mix-net (TM) contained in a voter-tallying module, and the method further comprises the step of using said first mix-net (TM) to apply ~~applying the~~ a decryption scheme (D_{TM}) which is an inverse [[to]] of said first encryption scheme to said data signal (x_i) at said voter-tallying module ~~whereby~~ to retrieve the ~~voter's~~ vote (v_i) of the voter.

4. (Currently Amended) The voting method of claim [[3]] 20, and comprising the steps of:

receiving, by a ballot-order-randomizing module, a batch of encrypted data signals (c_i) from said ballot-box module, said encrypted data signals being in a first order within said batch[[,]] ~~a batch~~ of encrypted data signals (c_i), each encrypted data signal (c_i) comprising data encrypted according to a second encryption scheme (E_M) and said data including a respective data signal (x_i), the encrypted data signal (c_i) including the vote (v_i) of the voter subjected to plural levels of encryption;

retrieving, in said ballot-order-randomizing module, each respective data signal (x_i) from the respective encrypted data signal (c_i) in said batch of encrypted data signals (c_i) by applying a decryption scheme (D_M) which is an inverse [[to]] of said second encryption scheme (E_M); ~~and~~

outputting the retrieved data signals (x_i) for said batch of encrypted data signals (c_i) in a different order from said first order; and

receiving, by said vote-tallying module, said retrieved data signals (x_i) in said different order.

5. (Currently Amended) The voting method of claim 4, wherein said second encryption scheme is the encryption scheme of a second mix-net (M) in said ballot-order-randomizing module, said second mix-net comprising a plurality of mix-servers.

6. (Currently Amended) The ~~electronic~~ voting method of claim 5, ~~and~~ further comprising the ~~step~~ steps of:

detecting irregularities in ~~the voting process, said step of detecting irregularities comprising verifying that the~~ one or more ballots to be counted do not contain duplicated data-pairs, wherein a data-pair corresponds to one of said data signals and the digital signature thereof for each of said one or more ballots, said mix-servers of said second mix-net (M) being prompted to generate zero-knowledge proofs of knowledge; and

if a particular mix-server (M_j) of said second mix-net (M) does not generate a satisfactory zero knowledge proof of the knowledge as a result of said prompting step, applying said decryption scheme (D_M) which is the inverse of said second encryption scheme (E_M) using said second mix-net (M) which excludes said particular mix-server (M_j) to retrieve said data signals (x_j).

7. (Currently Amended) The ~~electronic~~ voting method of claim [[5]] 20, ~~and~~ further comprising the ~~step~~ steps of:

comparing vote data held by the signer apparatus with vote data held by the ballot-box module to detect ~~detecting~~ irregularities in one or more of ~~the voting process, wherein the step of detecting irregularities comprises checking the validity of the digital signatures in~~ the ballots to be counted.

8. (Currently Amended) The ~~electronic~~ voting method of claim [[5]] 6, ~~and~~ further comprising the ~~step~~ steps of:

~~detecting irregularities in the voting process, wherein the step of detecting irregularities comprises checking that there is no overlap between the ballots to be counted and entries in a revocation list~~

controlling said trusted authority apparatus such that said tracing protocol of said fair blind signature scheme is applied to identify the signed data signals corresponding to said one or more ballots to be counted; and

including said identified signed data signals in a revocation list recording ballots that have been rejected.

9. (Currently Amended) ~~An electronic~~ The voting method ~~according to~~ of claim 1, ~~and~~ further comprising the steps of:

receiving said data signal (x_i) for the digital signature according to said fair blind signature scheme at a server module ~~(AS)~~ of said signer apparatus, said data signal (x_i) comprising [[a]] the vote (v_i) selected by [[a]] the voter (V_i), said vote (v_i) being encrypted according to ~~said~~ a first encryption scheme (E_{TM}), blinded according to said fair blind signature scheme and digitally signed according to a digital signature scheme of said voter;

verifying, by said server module ~~(AS)~~, that the digital signature (s_i) in the received data signal is valid;

in ~~the case~~ cases where the verifying step confirms that the digital signature in the data signal received by said server module ~~(AS)~~ is valid, said server module ~~(AS)~~ digitally signs the blinded encrypted vote (e_i) according to said fair blind digital scheme and outputs a ~~the~~ digitally-signed message ($S_{AS}(e_i)$);

unblinding the digitally-signed message ($S_{AS}(e_i)$) to yield said digital signature (y_i) of the data signal (x_i);

encrypting said data signal (x_i) and said digital signature (y_i) of the data signal thereof according to ~~said~~ a second encryption scheme (E_M) to produce an encrypted data signal (c_i); and

signing said encrypted data signal (c_i) according to [[a]] the digital signature scheme of the voter (V_i).

10. (Currently Amended) An electronic voting system comprising:

a plurality of voter modules each including a first processor; ~~(10)~~[[,]] and

an admin server module including a second processor; ~~(20),~~

wherein [[a]] the first processor, a voter module ~~(10)~~ and the second processor in the admin server module ~~(20)~~ cooperate ~~in~~ during a respective signing session in application of a fair blind signature scheme ~~whereby~~ to obtain, from said admin server module, a digital signature (y_i) of a data signal (x_i) from a voter module, said data signal (x_i) comprising ~~the~~ a respective ~~voter's~~ vote (v_i) of a voter, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated.

11. (Currently Amended) A voter module ~~(10) adapted~~ including a first processor configured to cooperate with a second processor in an admin server module ~~(20)~~ during a respective signing session in application of a fair blind signature scheme ~~whereby~~ to obtain, from

said admin server module, a digital signature (y_i) of a data signal (x_i) from the voter module, said data signal (x_i) comprising ~~the voter's~~ a vote (v_i) of a voter, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated.

12. (Currently Amended) A ~~computer~~ computer-readable medium encoded with a computer program executed by a computer that causes a first processor to cooperate with a second processor in an admin server module during a respective signing session in application of a fair blind signature scheme, the computer program comprising:

~~having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voter module (10) according to claim 11~~

program code for obtaining, from said admin server module, a digital signature (y_i) of a data signal (x_i), said data signal (x_i) comprising a vote (v_i) of a voter; and

program code for establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme.

13. (Currently Amended) A voting system admin server module including a first processor ~~(20) adapted~~ configured to cooperate with a second processor in a voter module during a respective signing session ~~(10)~~ in application of a fair blind signature scheme ~~whereby~~ to

obtain, from said admin server module, a digital signature (y_i) of a data signal (x_i) from said voter module, said data signal (x_i) comprising ~~the voter's~~ a vote (v_i) of a voter, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to link a given digitally-signed data signal with a signing session in which said digital signature was generated by said admin server module.

14. (Currently Amended) A computer-readable medium encoded with a computer program that causes a first processor to cooperate with a second processor in a voter module during a respective signing session in application of a fair blind signature scheme, the computer program comprising:

~~having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system admin server module (20) according to claim 13~~

program code for obtaining a digital signature (y_i) of a data signal (x_i) from said voter module, said data signal (x_i) comprising ~~the voter's~~ a vote (v_i) of a voter; and

program code for establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme.

15. (Currently Amended) A voting system ballot-order-randomizer ~~randomizer~~ module ~~(40)~~ comprising a processor configured to provide:

input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (c_i) comprising data (x_i) indicative of a respective ~~voter's~~ vote (v_i) of a voter which is digitally signed according to a fair blind signature scheme, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, each encrypted data signal (c_i) being encrypted according to a predetermined encryption scheme (E_M); ~~and~~

a mix-net (M) for decrypting said encrypted data signals (c_i) by applying a decryption scheme (D_M) which is an inverse [[to]] of said predetermined encryption scheme (E_M); and

output means for outputting the decrypted signals of said batch of cast votes in an order different from the order of ~~the~~ corresponding encrypted data signals in said batch of cast votes.

16. (Currently Amended) A computer-readable medium encoded with a computer program that causes a voting system ballot-order-randomizer to randomize a batch of cast votes, the computer program comprising:

~~having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system randomizer module (40) according to claim 15~~

program code for receiving, at an input means, a batch of cast votes, each cast vote comprising an encrypted data signal (c_i) comprising data (x_i) indicative of a respective vote (v_i) of a voter which is digitally signed according to a fair

blind signature scheme, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, each encrypted data signal (c_i) being encrypted according to a predetermined encryption scheme (E_M);

program code for decrypting, at a mix-net (M), said encrypted data signals (c_i) by applying a decryption scheme (D_M) which is an inverse of said predetermined encryption scheme (E_M); and

program code for outputting, at an output means, the decrypted signals of said batch of cast votes in an order different from the order of corresponding encrypted data signals in said batch of cast votes.

17. (Currently Amended) A voting system ~~tallier~~ tallying module ~~(50)~~ comprising a processor configured to provide:

input means for receiving cast votes, each cast vote comprising a data signal (x_i) digitally signed according to a fair blind signature scheme, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, each data signal (x_i) comprising a respective ~~voter's~~ vote (v_i) of a voter which is encrypted according to an encryption scheme (E_{TM}); and

a mix-net (M) for decrypting said encrypted votes (v_i) by applying a decryption scheme (D_{TM}) which is an inverse [[to]] of said encryption scheme (E_{TM}).

18. (Currently Amended) A computer-readable medium encoded with a computer program that causes tallying of cast votes, the computer program comprising:

~~having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system tallier module (50) according to claim 17~~

program code for receiving, at an input means, cast votes, each cast vote comprising a data signal (x_i) digitally signed according to a fair blind signature scheme, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, each data signal (x_i) comprising a respective vote (v_i) of a voter which is encrypted according to an encryption scheme (E_{TM}); and

program code for decrypting, at a mix-net (M), said encrypted votes (v_i) by applying a decryption scheme (D_{TM}) which is an inverse of said encryption scheme (E_{TM}).

19. (New) The voting method of claim 1, wherein the data signal (x_i) corresponds to the vote (v_i) of the voter which is encrypted according to a first encryption scheme (E_{TM}), said first encryption scheme comprising an encryption scheme of a vote-tallying module, and the method further comprising the step of applying a decryption scheme (D_{TM}) which is an inverse of said

first encryption scheme to said data signal (x_i) at said vote-tallying module to retrieve the vote (v_i) of the voter.

20. (New) The voting method of claim 19, further comprising the steps of:

setting a time period during which voting is authorized;

communicating a plurality of encrypted data signals (c_i) to a ballot-box module, each of said plural encrypted data signals (c_i) including data from a respective voter indicative of the vote (v_i) of said voter and digitally-signed by said signer apparatus; and

outputting, by said ballot-box module, said encrypted data signals (c_i) to said vote-tallying module after expiration of the time period in which voting is authorized.

21. (New) The voting method of claim 7, further comprising the steps of:

controlling said trusted authority apparatus such that said tracing protocol of said fair blind signature scheme is applied to identify signed data signals corresponding to said one or more of the ballots to be counted; and

including said identified signed data signals in a revocation list recording ballots that have been rejected.